AMENDMENTS TO CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (Withdrawn) A data carrier comprising:

a semiconductor chip having:

at least one memory;

an operating program stored in said memory; and

a plurality of operating program commands contained in said operating program, each command causing signals detectable from outside the semiconductor chip during execution of the command within the semiconductor chip,

wherein the data carrier is arranged to perform security-relevant operations solely by executing selected said operating program commands under one of the following conditions:

said selected operating program commands are operating program commands of such a kind that data processed with the corresponding program commands cannot be inferred from said signals that are caused by execution of said commands and that have been detected outside the semiconductor chip, or

said operating program commands are executed by the operating program in such a way that the data processed with the corresponding operating program commands cannot be inferred from said signals that are caused by execution of said commands and that have been detected outside the semiconductor chip.

2. (Withdrawn) A data carrier according to claim 1, wherein the executed operating program commands are designed for at least byte-by-byte processing of data.

3. (Withdrawn) A data carrier according to claim 1, wherein the operating program commands are selected such that the commands cannot be distinguished based on signal patterns caused thereby.

4. (Withdrawn) A data carrier according to claim 1, wherein the executed operating program commands each lead to a signal pattern which is substantially independent of the data processed with the corresponding command.

5. (Withdrawn) A data carrier according to claim 1, wherein the operating program is arranged to execute a series of operations (f), input data being required for executing the operations (f) and output data being generated by execution of the operations (f), said operations (f) including the following operations:

- falsification the input data by combination with auxiliary data (Z) before execution of one or more operations (f),
- combination of the output data determined by execution of the one or more operations (f) with an auxiliary function value ($f(Z)$) in order to compensate for the falsification of the input data,
- wherein the auxiliary function value ($f(Z)$) was previously determined by execution of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings and stored on the data carrier (1) along with the auxiliary data (Z).

6. (Withdrawn) A data carrier according to claim 5, wherein the combination with the auxiliary function values ($f(Z)$) for compensating the falsification is performed at the latest directly before execution of an operation (g) which is nonlinear with respect to the combination generating the falsification.

7. (Withdrawn) A data carrier according to claim 5, wherein the auxiliary data (Z) are varied, the corresponding function values being stored in the memory of the data carrier.

8. (Withdrawn) A data carrier according to claim 7, wherein new auxiliary values (Z) and new auxiliary function values ($f(Z)$) are generated by combining two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$).

9. (Withdrawn) A data carrier according to claim 8, wherein the two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$) intended for the combination are each selected randomly.

10. (Withdrawn) A data carrier according to claim 5, wherein pairs of auxiliary data (Z) and auxiliary function values ($f(Z)$) are generated by a generator without the operation ($f(Z)$) being applied to the auxiliary data (Z).

11. (Withdrawn) A data carrier according to claim 5, wherein the auxiliary data (Z) are a random number.

12. (Withdrawn) A data carrier according to claim 5, wherein the combination is an XOR operation.

13. (Withdrawn) A data carrier according to claim 1, wherein the operating program is arranged to execute a plurality of operations, wherein for at least a subset of said operations, the total result achieved by execution of several operations of the subset does not depend on the order of execution of the operations, and wherein the order of execution of the stated subset of operations is varied at least when the subset contains one or more security-relevant operations.

14. (Withdrawn) A data carrier according to claim 13, wherein the order of execution is varied at each run through the stated subset of operations.

15. (Withdrawn) A data carrier according to claim 13, wherein the order of execution is varied according to a fixed principle.

16. (Withdrawn) A data carrier according to claim 13, wherein the order of execution is varied randomly.

17. (Withdrawn) A data carrier according to claim 13, wherein the order of execution is varied in accordance with the data processed with the operations (*f*).

18. (Withdrawn) A data carrier according to claim 13, wherein the order of execution is fixed before execution of the first operation (*f*) of the subset for all operation of the subset whose execution is intended to be directly successive.

19. (Withdrawn) A data carrier according to claim 13, wherein, before the onset of execution of an operation (*f*) of the subset, the operation of the subset whose execution is intended to be successive and that is to be executed next, is fixed.

20. (Withdrawn) A data carrier according to claim 1, wherein the security-relevant operations are key permutations or permutations of other secret data.

21. (Withdrawn) A data carrier according to claim 1, wherein the data carrier is a smart card.

22. (Withdrawn) A method for executing security-relevant operations in a data carrier with a semiconductor chip having at least one memory in which an operating program containing a plurality of commands is stored, each command causing signals detectable from outside the semiconductor chip during execution of the command within the semiconductor chip, comprising the step of causing the data carrier to perform security-relevant operations (*f*) solely by executing said operating program commands, said step of causing the data carrier to perform security-relevant operations comprising one of the following steps:

executing only selected said operating program commands that are operating program commands of such a kind that data processed with the corresponding operating program

commands cannot be inferred from said signals that are caused by execution of said operating program commands and that have been detected outside the semiconductor chip, or

executing said operating program commands in such a way that the data processed with the corresponding operating program commands cannot be inferred from said signals that are caused by execution of said operating program commands and that have been detected outside the semiconductor chip.

23. (Withdrawn) A method according to claim 22, wherein the executed operating program commands employ data present at least byte by byte.

24. (Withdrawn) A method according to claim 22, wherein the operating program commands selected such that the commands cannot be distinguished based on signal patterns caused thereby.

25. (Withdrawn) A method according to claim 22, wherein the executed operating program commands each lead to a signal pattern which is substantially independent of the data processed with the command.

26. (Previously Presented) A method for protecting secret data serving as input data for one or more operations, comprising the steps of:

- falsifying the input data by combination with auxiliary data (Z) before execution of one or more operations (f),
- combining the output data determined by execution of the one or more operations (f) with an auxiliary function value ($f(Z)$) in order to compensate for the falsification of the input data,
- wherein the auxiliary function value ($f(Z)$) was previously determined by execution of the one or more operations (f) with the auxiliary data (Z) as input data in safe surroundings and stored along with the auxiliary data (Z).

27. (Previously Presented) A method according to claim 26, wherein the combination with the auxiliary function values ($f(Z)$) for compensating the falsification is performed at the latest directly before execution of an operation (g) which is nonlinear with respect to the combination generating the falsification.

28. (Previously Presented) A method according to claim 26, wherein the auxiliary data (Z) are varied, the corresponding function values being stored in a memory of a data carrier.

29. (Previously Presented) A method according to claim 28, wherein new auxiliary values (Z) and new auxiliary function values ($f(Z)$) are generated by combining two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$).

30. (Previously Presented) A method according to claim 29, wherein the two or more existing auxiliary data (Z) and auxiliary function values ($f(Z)$) that are combined to generate the new auxiliary values (Z) and new auxiliary function values ($f(Z)$) are each selected randomly.

31. (Previously Presented) A method according to claim 26, wherein pairs of auxiliary data (Z) and auxiliary function values ($f(Z)$) are generated by a generator without the operation ($f(Z)$) being applied to the auxiliary data (Z).

32. (Previously Presented) A method according to claim 26, wherein the auxiliary data (Z) are a random number.

33. (Previously Presented) A method according to claim 26, wherein the output data and the auxiliary function value are combined by an XOR operation.

34. (Withdrawn) A method for executing a plurality of operations (f) within the operating system of a data carrier, comprising the steps of:

executing the plurality of operations (*f*) in such a manner that, for at least a subset of said operations, the total result achieved by execution of several operations of the subset does not depend on the order of execution of the operations, and

varying the order of execution of the stated subset of operations at least when the subset contains one or more security-relevant operations.

35. (Withdrawn) A method according to claim 34, wherein the order of execution is varied at each run through the stated subset of operations.

36. (Withdrawn) A method according to claim 34, wherein the order of execution is varied according to a fixed principle.

37. (Withdrawn) A method according to claim 34, wherein the order of execution is varied randomly.

38. (Withdrawn) A method according to claim 34, wherein the order of execution is varied in accordance with the data processed with the operations (*f*).

39. (Withdrawn) A method according to claim 34, wherein the order of execution is fixed before execution of the first operation (*f*) of the subset for all operation of the subset whose execution is intended to be directly successive.

40. (Withdrawn) A method according to claim 35, further comprising the step of fixing, before the onset of execution of an operation (*f*) of the subset, which operation of the subset whose execution is intended to be successive is executed next.

41. (Withdrawn) A method according to claim 22, wherein the security-relevant operations are key permutations or permutations of other secret data.

42. (Previously Presented) A method according to claim 26, wherein the operations are key permutations or permutations of other secret data.

43. (Withdrawn) A method according to claim 34, wherein the security-relevant operations are key permutations or permutations of other secret data.